BIFID CIPHER

A classical cipher

Presented by   RIYA JANA

Historical Background :

- Bifid cipher is invented in 1895 by a French cryptographer, Felix Delastelle.
- Then after, he wrote his book named “Traite Elementaire de cryptographie” in 1901.
- Felix Delastelle introduced three more trifid cipher, four-square cipher and ADFGVX cipher.
- Bifid Cipher is combination of polybius square and transposition cipher.

Introduction:

- Bifid cipher encrypt messages by converting plain text into numeric coordinate based on a predetermined polybius square, it generates ciphertext by rearranging coordinates.
- It decrypt ciphertext into plain text using same polybius square, but it happens in reverse way.
- There will be a key that plays a vital role for creating polybius square.

Procedure:

Step1: Select any secrete key. For example, **DORAMON**.

Step 2: Take a plain text or Secrete Message, suppose **HELP ME OUT**.

Step 3: Make a polybius square starting with secrete key letters with no repetition. It is a 5x5 matrix.

Note: As alphabets are of 26 letters, J is skipped here. I and J considered as same letter.

Procedure:

Making a Polybius Square

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

ENCRYPTION

Plain text: HELP ME OUT

Row : 3234 12 144

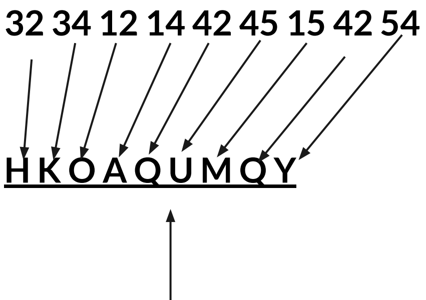
Column : 2451 54 254

Merging two coordinate one after another:

323412144245154254

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

After merging two coordinate one after another:



32 34 12 14 42 45 15 42 54

HKOAQUMQY

Now this encrypted message holding same length with plain text.

This will send to the receiver with the key.

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

DECRYPTION

At receiver's side, we have **H K O A Q U M Q Y** with the key DORAMON.

Here we need to take coordinates of each character of the cipher text.

CipherText: H K O A Q U M Q Y

Identify Coordinates:

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

CipherText: H **K** O A Q U M Q Y

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

CipherText: H K **O** A Q U M Q Y

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

CipherText: H K O **A** Q U M Q Y

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

CipherText: H K O A **Q** U M Q Y

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

CipherText: H K O A Q **U** M Q Y

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

CipherText: H K O A Q **U M** Q Y

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

CipherText: H K O A Q U M **Q** Y

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

CipherText: H K O A Q U M Q **Y**

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

After getting coordinates: 32 34 12 14 42 45 15 42 54

Decode it by dividing it into the length of ciphertext(9).

32 34 12 14 4 | 2 45 15 42 54

Row: 3 2 3 4 1 2 1 4 4

Column : 2 4 5 1 5 4 2 5 4

Decrypted Text : HELP ME OUT

	1	2	3	4	5
1	D	O	R	A	M
2	N	B	C	E	F
3	G	H	I	K	L
4	P	Q	S	T	U
5	V	W	X	Y	Z

THANK YOU